UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

PASCAL ABIDOR, et al. Plaintiffs, v. JANET NAPOLITANO, et al. Defendants	Civil Action No. 10 CV 4059 (Korman, J.) (Azrack, M.J.)

DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF MOTION TO DISMISS

TONY WEST
Assistant Attorney General

LORETTA E. LYNCH
United States Attorney

ELLIOT M. SCHACHNER
Assistant U.S. Attorney

SANDRA M. SCHRAIBMAN
Assistant Branch Director

MARCIA SOWLES
Senior Counsel
U.S. Department of Justice, Civil Division
Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7114
Washington, D.C. 20530
Tel.: (202) 514-4960
Fax.: (202) 616-8470
Email: marcia.sowles@usdoj.gov

TABLE OF CONTENTS

PRELIMINARY STATEMENT

The Supreme Court has held that "[r]outine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause or warrant." *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004) (quoting *United States v. Montonya de Hernandez*, 473 U.S. 531, 538 (1985)). Based on this long standing, well-established legal authority of the Government to conduct broad searches at the border, two U.S. Department of Homeland Security ("DHS") components, U.S. Customs and Border Protection ("CBP") and U.S. Immigration and Customs Enforcement ("ICE"), issued policies providing guidelines for officers and agents conducting border searches of information contained in electronic devices. The policies, issued in August 2009, and which were made available to the public, reflect the Government's conscientious effort to "strike the balance between respecting the civil liberties and privacy of all travelers while ensuring DHS can take the lawful actions necessary to secure our borders."[1]

In this action, Plaintiffs Pascal Abidor, the National Association of Criminal Defense Lawyers ("NACDL"), and the National Press Photographers Association ("NPPA") challenge these policies. They assert that the policies violate their First and Fourth Amendment rights "by permitting the suspicionless search, copying, and detention of electronic devices" that may contain "expressive, protected materials." Compl., ¶¶ 128-129. Plaintiffs ask the Court to declare the policies facially invalid and enjoin Defendants from permitting any searches of electronic devices without demonstrating reasonable suspicion. In addition, Abidor seeks a declaration that the border search of his laptop and external hard drive in May 2010 violated the

---

[1] *See* Secretary Napolitano Announces New Directives on Border Searches of Electronic Media (Aug. 27, 2009) ("August 2009 Press Release"), *available at* www.dhs.gov/ynews/releases/pr_1251393255852.shtm.

First and Fourth Amendments.

Plaintiffs' complaint should be dismissed on two grounds. First, Plaintiffs' facial challenge to the policies should be dismissed for lack of subject matter jurisdiction pursuant to Fed. R. Civ. P. 12(b)(1) because Plaintiffs lack standing to obtain the declaratory and injunctive relief that they seek. To establish standing under Article III of the Constitution, Plaintiffs have the burden of showing, *inter alia*, that their alleged injury is likely to be redressed by the relief that they seek. Past exposure to alleged illegal conduct is not sufficient for either declaratory or injunctive relief. Instead, Plaintiff are required to show "a real and immediate threat" that such alleged illegal acts will be repeated in the future. *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983). Plaintiffs cannot meet this requirement. Plaintiffs' bald assertion that their electronic devices are "likely" to be searched in the near future is pure speculation, and fails to demonstrate the type of concrete and imminent injury necessary for Article III standing.

Second, all of Plaintiffs' claims should be dismissed on the merits for failure to state a claim pursuant to Fed. R. Civ. P. 12(b)(6). Plaintiffs' Fourth Amendment claims have no merit. Recognizing that electronic devices are similar to luggage and other closed containers, courts have repeatedly held that customs officials are entitled to inspect the contents of such devices without showing particularized suspicion. *See infra.* at 20-21. Plaintiffs' First Amendment challenge likewise has no merit. Courts have found that an otherwise valid border search under the Fourth Amendment does not violate the First Amendment rights of an individual simply because the search uncovers expressive materials. *See infra* at 27-28. Indeed, both the Fourth and Ninth Circuits have explicitly rejected claims that a different rule should be applied to laptops or other electronic devices.

Accordingly, Defendants respectfully request that the Court dismiss the complaint in its

entirety.

BACKGROUND

I. The Government's Authority to Conduct Border Searches

"[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *United States v. Flores-Montano*, 541 U.S. at 153. "The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border. Time and again, we have stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'" *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)).

DHS, through its components CBP and ICE, is the first line of defense at the border, responsible for administering the customs and immigration laws of the United States, securing the borders, and inspecting individuals and items that seek entry into and propose exit from the United States. *See* 6 U.S.C. §§ 202(2), (4) & (6). One of DHS' most important responsibilities is "preventing the entry of terrorists and the instruments of terrorism into the United States." 6 U.S.C. §§ 111(b)(1)(A), 202(1). In addition, DHS is also responsible for enforcing hundreds of laws and regulations, including those addressing immigration, currency and financial transactions, customs, commerce and trade, copyrights and trademarks, narcotics, the safety of agricultural products and other goods, and import and export controls on wildlife and plants, chemical and biological weapons, guns, and other items.[2]

---

[2] *See generally* Summary of Laws and Regulations Enforced by CBP (2005), *available at*
(continued...)

In light of these numerous, varied and important responsibilities, for more than two centuries, Government officers have exercised broad authority to inspect travelers and their baggage as they cross the international border. *See* Act of July 31, 1789, ch. 5, 1 Stat. 29; *see also*, *e.g.*, 8 U.S.C. § 1357 (authority of immigration officers to board and search); 19 U.S.C. §§ 482 (authority to search vehicles and persons), 1461 (authority to search "[a]ll merchandise and baggage" brought into the United States), 1496 (authority to search baggage of persons entering the United States), 1499(a) (authority to examine and detain imported merchandise), 1305 (authority to search for potentially obscene material), 1581 (authority to board vessels and search), 1582 (authority to detain and search "all persons coming into the United States from foreign countries"), 1583 (authority to examine outbound mail), 1589a (general law enforcement authority), 1595a(c)(3) (authority to detain merchandise introduced contrary to law); 31 U.S.C. § 5317 (authority regarding search and forfeiture of monetary instruments); 15 C.F.R. § 758.7; 19 C.F.R. §§ 162.6 and 162.7.

Border searches of electronic devices are "a crucial tool for detecting information relating to terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband including child pornography; laundering monetary instruments; violations of copyright or trademark laws; and evidence of embargo violations or other import or export control laws." ICE Directive No. 7-6.1 ("ICE Directive"), ¶ 4 (attached as Exhibit A); *see also* CBP Directive No. 3340-049 ("CBP Directive") (attached as Exhibit B), ¶ 1; August 2009 Press Release, at 1 ("Searches of electronic media, permitted by law and carried out at borders and

---

[2](...continued)
http://www.cbp.gov/xp/cgov/trade/legal/summary_laws_enforced/: these same laws and regulations are investigated and prosecuted by ICE.

ports of entry, are vital to detecting information that poses serious harm to the United States, including terrorist plans, or constitutes criminal activity – such as possession of child pornography and trademark or copyright infringement.") (attached as Exhibit C).

In August 2009, CBP and ICE issued policies providing guidelines for conducting border searches of electronic devices. *See* Exhibits A and B. As described below, these policies have been carefully crafted to provide the Government, through DHS and its components, with the tools necessary to secure the nation's border, while striving to protect personal privacy to the greatest extent possible.

A. Searching Electronic Devices at the International Border

The challenged policies relate exclusively to border searches – that is, searches of individual traveler's electronic devices performed at the international border by properly authorized CBP officers or ICE agents (hereinafter "customs officers"). *See* CBP Directive, ¶¶ 2.2, 3.1, 5.1.1; ICE Directive, ¶¶ 1.1, 8.1(1). Generally, a border search of an electronic device will be initiated by a CBP officer, who may provide the device or a copy of its contents to an ICE agent "for analysis and investigation." CBP Directive, ¶ 2.7; *see also* ICE Directive, ¶ 7.4. The policies permit customs officers to search, analyze, and review information contained in electronic devices "with or without individualized suspicion," subject to the guidelines set forth in the policy directives and any other applicable laws. *See* CBP Directive, ¶ 5.1.2; ICE Directive, ¶ 6.1. Such searches should be performed in the presence of the traveler, "unless there are national security, law enforcement, or other operational considerations that make it inappropriate to permit the individual to remain present." CBP Directive, ¶ 5.1.4; *see also* ICE Directive, ¶ 8.1(2).

The policies recognize that it is not always possible to complete the search of a traveler's

electronic device while he or she waits at the border, not only for operational reasons as noted above, but also for the convenience of the traveler. Accordingly, customs officers are permitted to "detain electronic devices, or copies of information contained therein, for a brief, reasonable period of time to perform a thorough border search." CBP Directive, ¶ 5.3.1; *see also* ICE Directive, ¶ 8.3.1. If CBP officials detain an electronic device, they must provide the traveler with a receipt and, unless doing so would hamper national security or law enforcement or operational concerns, must notify the traveler "of the purpose and authority for these types of searches, how the individual may obtain more information on reporting concerns about their search, and how the individual may seek redress from the agency if he or she feels aggrieved by a search." CBP Directive, ¶¶ 5.3.1.3, 5.3.1.4.

By policy, if CBP conducts a search of a detained device, the search must be completed "as expeditiously as possible" (ordinarily within five days). CBP Directive, ¶ 5.3.1. This period may be extended to fifteen days only with the approval of the Port Director or an official of similar rank. *Id.* Any further extensions require approval at the Director of Field Operations level. *Id.* If CBP turns over a detained electronic device to ICE for "analysis and investigation," ICE policy also requires its agents "to complete the search of [a] detained electronic device[], or copies of information therefrom, in a reasonable time given the facts and circumstances of the particular search." ICE Directive, ¶¶ 6.2, 8.3(1).[3] The ICE Directive provides that such searches are generally to be completed within thirty calendar days of the date of the detention, unless circumstances exist that warrant more time. *Id.* ¶ 8.3(1).

---

[3] When CBP detains, seizes, or retains an electronic device (or copies of information therefrom), and turns such over to ICE for analysis and investigation, ICE policy will apply once it is received by ICE. *See* CBP Directive, ¶ 2.7; ICE Directive, ¶ 6.2.

B. Seeking Assistance to Search Electronic Devices

Customs officers have the right to demand assistance from any individual to assist in a border search. *See* 19 U.S.C. § 507. Recognizing that customs officers may encounter technical difficulties, encrypted information, or information in a foreign language that would preclude the effective search of an electronic device, the policies permit customs officers to seek translation, encryption, and/or other technical assistance, without individualized suspicion. *See* CBP Directive, ¶ 5.3.2.2; *see also* ICE Directive, ¶ 8.4(1). By contrast, the policies provide that customs officers may seek subject matter assistance from other federal agencies – *i.e.*, assistance with the "meaning, context, or value of information" contained on the electronic device -- if the officers possess reasonable suspicion that the information relates to laws enforced by DHS. CBP Directive, ¶ 5.3.2.3; *see also* ICE Directive, ¶ 8.4(2).

C. Handling Sensitive Information in Electronic Devices

The policies contain special provisions for the treatment of privileged or other sensitive information encountered during the border search of electronic devices. For example, the policies recognize that confidential business information requires special handling, and that its disclosure by customs officials may be restricted by law, including the Trade Secrets Act (18 U.S.C. § 1905). *See* CBP Directive, ¶ 5.2.3; ICE Directive, ¶ 8.6.(2)(a). The policies also require other potentially sensitive information, such as medical records or work-related information carried by journalists, to be handled in accordance with applicable federal law and policy, and direct customs officers to consult with their Chief Counsel's office if they have questions or concerns. *See* CBP Directive, ¶ 5.2.2; ICE Directive, ¶ 8.6(2)(c).

Finally, the policies recognize that customs officers may discover information subject to protection by either the attorney-client privilege or the attorney work-product doctrine. If such

information constitutes evidence of a crime or otherwise pertains to a determination within the jurisdiction of CBP or ICE, the customs officers conducting the search are directed to seek advice from the CBP or ICE Chief Counsel's office or the appropriate U.S. Attorney's office to ensure that an appropriate procedure is utilized. *See* CBP Directive, ¶ 5.2.1; ICE Directive, ¶ 8.6(2)(b).

D. Retention of Electronic Devices and Information

Once the border search of an electronic device is complete, the policies permit customs officers to "seize and retain an electronic device, or copies of the information from the device, when, based on a review of the electronic device encountered or on other facts and circumstances, they determine there is probable cause to believe that the device, or copy of the contents thereof, contains evidence of or is the fruit of a crime." CBP Directive, ¶ 5.4.1.1; *see also* ICE Directive, ¶ 8.5(1)(a) (same). Except as otherwise provided, if customs officers determine that probable cause for a seizure does not exist, any detained electronic device will be returned to the traveler, and any copies of the information contained therein—including any sensitive or privileged information—will be destroyed. *See* CBP Directive, ¶¶ 5.3.1.2, 5.3.3.4, 5.4.1.6; ICE Directive, ¶¶ 8.1(5), 8.5(1)(e), 8.5(2)(b).[4]

[4] Without probable cause to seize an electronic device, CBP may retain only information relating to immigration, customs, and other enforcement matters if such retention is consistent with the privacy and data protection standards of the system of records in which such information is retained. CBP Directive, ¶ 5.4.1.2. Similarly, to the extent authorized by law, ICE may retain information relevant to immigration, customs, and other law enforcement matters in ICE systems if such retention is consistent with the privacy and data protection policies of the system in which such information is retained. ICE Directive, ¶ 8.5(1)(b).

II. Plaintiffs' Allegations[5]

A. Pascal Abidor

On May 1, 2010, Plaintiff Pascal Abidor, a United States and French dual citizen, boarded a train in Montreal destined for Brooklyn. *See* Compl., ¶¶ 7, 24. He provided his U.S. passport to, and was questioned by, a CBP officer when he reached the inspection point in the vicinity of Service Port-Champlain. *See id.*, ¶¶ 25-26. In response to questions, Abidor stated that he is a graduate student pursuing a degree in Islamic studies, and that he had lived in Jordan and visited Lebanon during the past year. *See id.*, ¶¶ 27-28. He provided the CBP officer with his French passport, which contained visas for Jordan and Lebanon, and the officer subsequently escorted Abidor to the café car. *See id.*, ¶ 29. In the presence of Abidor and other CBP officers, the officer performed a brief initial border search of Abidor's laptop and discovered images of Hamas and Hezbollah rallies.[6] *See id.*, ¶¶ 30-32. Abidor stated that such photographs were relevant to his area of study, the modern history of Shiites in Lebanon. *See id.*, ¶ 32. The CBP officers asked Abidor to write down the password for his laptop and a few more general questions regarding his associations, his area of study, where he had lived in the past four years, and his plans for the future. *See id.*, ¶ 33.

Abidor was then escorted to the Port of Champlain and questioned for approximately three hours. *See id.*, ¶ ¶ 35-36. Abidor left the port at approximately 4:00 p.m., but his laptop and external hard drive were detained by CBP, which provided Abidor a Detention Notice and Custody Receipt for Detained Property. *See id.*, ¶¶ 42-43, 45. The receipt "indicated that the

---

[5] These allegations are accepted as true only for purposes of resolving the Government's motion to dismiss.

[6] These organizations are listed in the U.S. Department of State's list of foreign terrorist organizations. *See* http://www.state.gov/s/ct/rls/other/des/123085.htm.

devices were being held for ICE." *Id.*, ¶ 43. Abidor further alleges that his laptop was searched while he was questioned at the port and during the period between May 1, 2010, and when he received his laptop on May 12, 2010. *See id.*, ¶¶ 41, 50-51. Abidor also alleges, on information and belief, that officers from CBP, ICE, and/or other agencies copied the contents of his laptop and external hard drive and continue to retain such copies. *See id.*, ¶ 52-54.

Abidor alleges that he will continue to travel frequently across the U.S. border with his electronic devices. *See id.*, ¶ 55. He admits, however, that his electronic devices were not searched on July 8, 2010, when he returned from a trip to Europe just two months after the alleged search that occurred during his trip to New York. *See id.*, ¶ 58. Abidor does not allege that information derived from his laptop has been improperly disclosed; however, he claims that he has altered his behavior in order to avoid the possibility that information on his laptop will be "misconstrued" if it is ever searched again. *Id.*, ¶¶ 62, 63.

B. National Association of Criminal Defense Lawyers

The National Association of Criminal Defense Lawyers ("NACDL") sues on behalf of its 10,000 members, alleging that "many" of its members travel abroad in the course of their representation of their clients and bring their electronic devices with them. *Id.*, ¶¶ 8, 66, 69, 70. NACDL "fears that its members' electronic devices will be searched, copied, and detained by U.S. border officials under the ICE and CBP policies." *Id.*, ¶ 84.

In an attempt to substantiate this alleged fear, NACDL points to a single instance in which one of its members was, it presumes, subject to a "suspicionless search of her laptop." *Id.*, ¶ 85. The organization alleges that, in August 2008, one year before the challenged policies were issued, NACDL's President-Elect Lisa Wayne was subject to a secondary inspection, during which a "CBP officer took Ms. Wayne's computer out of sight for more than 30 minutes,

presumably to complete an electronic search." *Id.*, ¶ 95.

C. National Press Photographers Association

The National Press Photographers Association ("NPPA") sues on behalf of its 7,000 members, alleging that many of its members travel abroad, and that they often "travel with electronic devices that are necessary for them to carry out their work." *Id.*, ¶¶ 100, 102, 107. As a result, "NPPA fears that its members' electronic devices will be searched, copied, and detained by U.S. border officials under the CBP and ICE policies." *Id.*, ¶ 119.

Like NACDL, NPPA cites a single example to justify this alleged fear. *Id.*, ¶¶ 120-127. In July 2007, more than two years before the challenged policies were issued, Duane Kerzic crossed the United States border from Canada. *Id.*, ¶ 122. NPPA alleges that, CBP officers referred Kerzic to secondary screening at the inspection point, and one CBP officer looked at his laptop for fifteen minutes before returning it to Mr. Kerzic and admitting him to the United States. *Id.*, ¶ 125. Although, "Kerzic travels frequently across the U.S. border with his electronic devices[,]" *id.*, ¶ 127, this fifteen minute inspection of his laptop is the only time Plaintiffs allege his laptop has been searched.

D. Claims and Prayer for Relief

Plaintiffs' complaint contains two causes of action. In the first cause of action, all three Plaintiffs raise a facial challenge to the policies. They claim that the policies violate their First and Fourth Amendment rights "by permitting the suspicionless search, copying, and detention of electronic devices" that may contain "expressive, protected materials." *Id.*, ¶¶ 128-129. They ask the Court to declare the policies unconstitutional and to "[e]njoin defendants from enforcing their policies of searching, copying, and detaining electronic devices at the international border without reasonable suspicion." *Id.*, Prayer for Relief, ¶¶ A, B, D. In the second cause of action,

Plaintiff Abidor challenges the May 2010 border search of his laptop and external hard drive, and claims that the search of the electronic devices violated his First and Fourth Amendment rights. *See id.*, ¶¶ 130-131. He seeks a declaration that this search was unconstitutional, and an order directing Defendants to return or destroy any information unlawfully obtained from him. *See id.*, Prayer for Relief, ¶¶ C, F.

STANDARD OF REVIEW

Federal Rule of Civil Procedure 12(b)(1) allows Defendants to challenge the Court's subject matter jurisdiction by means of a motion to dismiss. In reviewing a motion to dismiss under Rule 12(b)(1), the Court must "accept as true all material factual allegations in the complaint[,]" but also must refrain from "drawing from the pleadings inferences favorable to the party asserting [jurisdiction]." *Shipping Fin. Servs. Corp. v. Drakos*, 140 F.3d 129, 131 (2d Cir. 1998) (citations omitted). Furthermore, a district court may consider affidavits and other materials outside the pleadings when resolving a motion to dismiss for lack of subject-matter jurisdiction without converting the motion to dismiss into a motion for summary judgment. *Alliance for Envtl. Renewal, Inc. v. Pyramid Crossgates Co.*, 436 F.3d 82, 88 n.8 (2d Cir. 2006).

Federal Rule of Civil Procedure 12(b)(6) allows Defendants to challenge the legal sufficiency of Plaintiffs' claims. In order to survive a motion to dismiss, the complaint must allege a plausible set of facts sufficient "to raise a right to relief above the speculative level." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007); *accord Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949-50 (2009). In ruling on a Rule 12(b)(6) motion, the Court may consider the complaint, documents that are incorporated by reference or integral to the complaint, and matters of which judicial notice may be taken. *See, e.g., Zynger v. Dep't. of Homeland Sec.*, 615 F. Supp. 2d 50, 61 (E.D.N.Y. 2009) (citing *Chambers v. Time Warner, Inc.*, 282 F.3d 147, 152 (2d

Cir. 2002) and *Kramer v. Time Warner, Inc.*, 937 F.2d 767, 773 (2d Cir. 1991)).

ARGUMENT

I. PLAINTIFFS' FACIAL CHALLENGE TO THE POLICIES SHOULD BE DISMISSED FOR LACK OF STANDING.

Before addressing the merits of Plaintiffs' facial constitutional challenge to CBP's and ICE's policies, the Court must first determine whether Plaintiffs have standing to obtain the declaratory and injunctive relief they seek. *See DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) ("[A] plaintiff must demonstrate standing separately for each form of relief sought."). Plaintiffs do not have the requisite standing.

Article III of the Constitution "confines the federal courts to adjudicating actual 'cases' and 'controversies.'" *Allen v. Wright*, 468 U.S. 737, 750 (1984). This is a "bedrock requirement." *Valley Forge Christian College v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 471 (1982). Indeed, "[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies." *Simon v. Eastern Ky. Welfare Rights Org*, 426 U.S. 26, 37 (1976). A court's standing inquiry is "especially rigorous when reaching the merits of the dispute would force [the court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." *Raines v. Byrd*, 521 U.S. 811, 819-20 (1997).

A federal court must presume that it "lack[s] jurisdiction unless the contrary appears affirmatively from the record." *Renne v. Geary*, 501 U.S. 312, 316 (1991) (internal quotation marks omitted). Thus, it is a plaintiff's burden, as the party asserting the court's jurisdiction, to establish his standing to bring suit. *See DaimlerChrysler Corp.*, 547 U.S. at 342. To establish

standing, a plaintiff must "demonstrate the now-familiar elements of injury in fact, causation and redressability." *Lance v. Coffman*, 549 U.S. 437, 439 (2007). Plaintiffs must show "personal injury fairly traceable to defendant's allegedly unlawful conduct and likely to be redressed by the requested relief." *DaimlerChrysler Corp.*, 547 U.S. at 342 (quoting *Allen*, 468 U.S. at 751). Where, as here, an organization brings suit on behalf of its members, it has standing only if "its members would otherwise have standing to sue in their own right, the interests at stake are germane to the organization's purpose, and neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 181 (2000).

To establish injury in fact, a plaintiff must show "an invasion of a legally protected interest" which is both (1) "concrete and particularized," and (2) "actual or imminent, not conjectural or hypothetical." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (internal quotation marks omitted). The Supreme Court has "consistently held that a plaintiff raising only a generally available grievance about government – claiming only harm to his and every citizen's interest in proper application of the Constitution and laws, and seeking relief that no more directly and tangibly benefits him than it does the public at large – does not state an Article III case or controversy." *Id.* at 573-74.

While past exposure to alleged illegal acts may be sufficient to establish standing for damages (which none of the Plaintiffs seek in this case), it is not sufficient to establish standing for the prospective declaratory and injunctive relief which Plaintiffs seek here. Instead, to seek declaratory or injunctive relief, plaintiffs must first establish that they are "'immediately in danger of sustaining some direct injury as [a] result of the challenged [policies].'" *Shain v. Ellison*, 356 F.3d 211, 215 (2d Cir. 2004) (quoting *City of Los Angeles v. Lyons*, 461 U.S. 95,

101-02 (1983)). Thus, "the critical standing inquiry is whether a plaintiff is 'realistically threatened by a repetition of his experience . . .' or whether the claim is 'speculative.'" *Curtis v. City of New Haven*, 726 F.2d 65, 67 (2d Cir. 1984) (quoting *Lyons*, 461 U.S. at 109).

For example, in *City of Los Angeles v. Lyons*, the Supreme Court held that Lyons, who had been subject to a stranglehold by the Los Angeles police, would have standing to seek to enjoin an alleged policy permitting the use of strangleholds only if he could show that he "would again be stopped for a traffic or other violation *in the reasonably near future,*" and "that strangleholds are applied by the Los Angeles police to *every citizen who is stopped* or arrested regardless of the conduct of the person stopped." *Lyons*, 461 U.S. at 108 (emphasis added). The Supreme Court found that "the odds" of this happening were not "sufficient to make out a federal case for equitable relief[,]" in part because "five months elapsed between [the past incident] and the filing of the complaint, yet there was no allegation of further unfortunate encounters between Lyons and the police." *Id.*

In this case, Plaintiffs cannot show that they are "immediately in danger of sustaining some direct injury as [a] result of the challenged [policies]." *Id.* at 101-02 (internal quotations and citations omitted). While Abidor alleges that he frequently travels internationally with electronic devices, he points to only a single, isolated instance on May 1, 2010, in which he claims that his electronic devices were searched at the border. *See* Compl., ¶¶ 20, 30-54. In fact, he admits that he has traveled internationally at least once since that date and did not have his electronic devices searched at the border. *See id.* ¶ 58. Therefore, in this case, as in *Lyons,* more than a few months elapsed between the alleged incident involving Abidor and the filing of the complaint. Abidor does not allege that he has been confronted with any further searches of his electronic devices, despite his admission to being subject to inspection once when he re-entered

the United States in July 2010. *See* Compl., ¶ 58. Likewise, while NACDL and NPPA allege that their members frequently travel internationally with electronic devices, NACDL and NPPA identify only two instances – one in 2007 and one in 2008, before the challenged policies were issued – in which they allege that any of their members had their electronic devices searched. *See id.* ¶¶ 94, 125.

Indeed, even the statistics alleged by Plaintiffs in their Complaint demonstrate that border searches of electronic devices are extremely rare.[7] Although approximately 590 million persons crossed the border into the United States between October 1, 2008, and June 2, 2010 (*see* Declaration of Troy Riley, ¶ 4 (hereinafter "Riley Decl.") (attached as Exhibit D),[8] Plaintiffs allege that only 6,500 persons were subjected to searches of their electronic devices. *See* Compl., ¶ 1. Thus, even assuming that all of these searches occurred on inbound travelers to the United States, there was only one such search for every 90,000 inbound travelers; in other words approximately 0.0011% of the travelers were subjected to this type of search at the border. Moreover, as Plaintiffs allege, of the 6,500 persons who had electronic devices searched, the electronic devices were detained in only 220 cases. *Id.* ¶ 20. Assuming that all of these cases involved inbound travelers, this represents approximately one detention for every 2.6 million inbound travelers, or 0.000038% of those travelers. Therefore, Plaintiffs' professed fears that Abidor or NACDL and NPPA members (for which the Complaint makes no allegation about any

[7] While the rarity of the border searches of electronic devices supports our jurisdictional argument on standing, the constitutionality of border searches of electronic devices does not rest on the frequency with which such searches are conducted.

[8] Although the Government has authority to conduct borders searches of outbound travelers as well as inbound travelers, *see, e.g., United States v. Swarovski*, 592 F.2d 131, 133 (2d Cir. 1979), CBP does not process all travelers who depart the United States through a port of entry; CBP's record systems do not indicate the total number of *outbound* travelers during this period. *See* Riley Decl., ¶ 5.

searches conducted after the challenged policies were issued) likely will be subject to future searches of their electronic devices are purely speculative, and thus do not give them standing to challenge the policies by seeking declaratory and injunctive relief.

Plaintiffs' allegations that they have altered their behavior due to the entirely speculative possibility that their electronic media may someday be subject to a suspicionless search – *see, e.g.,* Compl., ¶¶ 62, 63, 83, 116 – are insufficient to establish standing. A party's subjective fears, even if accompanied by changes in conduct, "are not an adequate substitute for a claim of specific present objective harm or a threat of future harm." *Laird v. Tatum*, 408 U.S. 1, 14 (1972); *see also White v. United States*, 601 F.3d 545, 554 (6th Cir. 2010); *Nat'l Council of La Raza v. Gonzales*, 468 F. Supp. 2d 429, 443-44 (E.D.N.Y. 2007), *aff'd* 283 Fed. App. 848 (2d Cir. 2008). Where, as here, there is no reasonable likelihood of future harm to plaintiffs who challenge government action, they may not rely on their changes in conduct to confer standing upon themselves. "In the standing context the indirect harm of a chilling effect on speech [or behavior] may only be asserted in conjunction with a danger of direct harm from the challenged statute, because that danger is the source of the chill." *Amnesty Int'l USA v. McConnell*, 646 F. Supp. 2d 633, 654 (S.D.N.Y. 2009).

A contrary rule would allow plaintiffs to evade Article III's standing requirements by altering their behavior based on a subjectively perceived (but objectively unreasonable) fear that they will be subject to the challenged government action. The Supreme Court has made it clear that a plaintiff's subjective fears are insufficient to confer standing. "The reasonableness of [P]laintiffs' fear is dependent upon the likelihood of a recurrence of the allegedly unlawful conduct. It is the *reality* of the threat of repeated injury that is relevant to the standing inquiry, not the [Plaintiffs'] subjective apprehensions." *Lyons*, 461 U.S. at 107 n.8 (emphasis added).

Accordingly, because it is entirely speculative that Plaintiffs will be subject to any border search conducted in accordance with the challenged policies again in the future, let alone a search not based on suspicion, the derivative harm – the present alteration of their behavior – cannot support Plaintiffs' standing.

II. THE POLICIES REGARDING BORDER SEARCHES OF ELECTRONIC DEVICES DO NOT VIOLATE THE CONSTITUTION ON THEIR FACE.

Assuming *arguendo* that the Court has jurisdiction to hear Plaintiffs' claims for declaratory and injunctive relief, Plaintiffs' facial challenges to Defendants' policies regarding border searches of laptops and other electronic devices (*See* Compl., ¶¶ 128-129) should be dismissed pursuant to Fed. R. Civ. P. 12(b)(6) for failure to state a claim. Plaintiffs' request for prospective declaratory and injunctive relief with respect to the challenged policies does not concern a particular "search or seizure," but challenges the "suspicionless search, copying, and detention of electronic devices" in the abstract. *See* Compl., ¶ 128. In order to invalidate the challenged policies on their face, Plaintiffs must shoulder a heavy burden. "To prevail in such a facial challenge, [Plaintiffs] 'must establish that no set of circumstances exists under which the [policies] would be valid.'" *Reno v. Flores*, 507 U.S. 292, 301 (1993) (quoting *United States v. Salerno*, 481 U.S. 739, 745 (1987)); *see also New York State Nat'l Org. for Women v. Pataki*, 261 F.3d 156, 171 (2d Cir. 2001). Plaintiffs cannot carry their burden.

A. The Policies Do Not Violate the Fourth Amendment.

Plaintiffs' claim that the suspicionless search of the contents of laptops and other electronic devices at the border violates the Fourth Amendment has no merit. The Fourth Amendment requires only "that searches and seizures be reasonable." *Montoya de Hernandez*, 473 U.S. at 537. "[T]he Fourth Amendment's balance of reasonableness is qualitatively different

at the international border than in the interior." *Id.* at 538. "[T]he United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *Flores-Montano*, 541 U.S. at 153. Indeed, the Supreme Court has stressed that "the Government's interest in preventing the entry of unwanted persons and effects is at its *zenith* at the international border." *Id.* at 152 (emphasis added). For this reason, it has long been acknowledged that "'searches made at the border, pursuant to the long standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'" *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)). Indeed, the border search doctrine, which permits suspicionless searches of those persons and things crossing the border, has a history as old as the Fourth Amendment itself. *See id.* at 153 (stating that the Government's authority to conduct warrantless searches at the border has an "impressive historical pedigree").

Accordingly, the Supreme Court has held that "[r]outine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . . ." *Montoya de Hernandez*, 473 U.S. at 538. While a narrow category of *personal* searches, "'such as strip, body cavity, or involuntary x-ray searches[,]" may require reasonable suspicion, *id.* at 541 n. 4, the Supreme Court has explicitly rejected attempts to extend this exception beyond "highly intrusive searches *of the person*." *Flores-Montano*, 541 U.S. at 152 (holding that complete disassembly and reassembly of a car gas tank did not require particularized suspicion) (emphasis added); *accord Rahman v. Chertoff*, 530 F.3d 622, 624 (7th Cir. 2008) (holding only "stops that entail intrusive searches of the body are in a special category"). Hence, when a border search of property (rather than a search of a person) is in question, no balancing must be done to determine whether the search was routine. *See*

Flores v. Montano, 541 U.S. at 152.

"Courts have long held that searches of closed containers and their contents can be conducted at the border without particularized suspicion under the Fourth Amendment." *United States v. Arnold*, 533 F.3d 1003, 1007 (9th Cir. 2008), *cert. denied* 129 S. Ct. 1312 (2009); *see also United States v. Irving*, No. 03-cr-633, 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003) ("Inspection of the contents of closed containers comes within the scope of a routine border search and is permissible even in the absence of reasonable suspicion or probable cause."), *aff'd*, 452 F.3d 110 (2d Cir. 2006). Thus, the Second Circuit has "long ruled that searches of a person's luggage . . . are routine searches." *United States v. Irving*, 452 F.3d at 123-24 (citing *United States v. Asbury*, 586 F.2d 973, 975 (2d Cir. 1978)).

Like luggage, electronic devices are classified as closed containers for Fourth Amendment purposes. *United States v. Irving*, 2003 WL 22127913, at *5 ("Several courts have compared personal notebook computers to closed containers for the purposes of the Fourth Amendment analysis", citing, *inter alia*, *United States v. Runyan*, 275 F.3d 449, 458 (5th Cir. 2001), and *United States v. Al-Marri*, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002)); *United States v. McAuley*, 563 F. Supp. 2d 672, 677 (W.D. Tex. 2008) ("Relying on the Supreme Court's reasoning in *Flores-Montano*, this Court cannot equate the search of a computer with the search of a person. The Court finds that the search of a computer is more analogous to the search of a vehicle and/or its contents.").

Because laptop computers and other electronic devices are considered to be closed containers, courts have repeatedly held that customs officers are "entitled to inspect the contents of the [electronic devices] even absent reasonable suspicion." *Irving*, 2003 WL 22127913, at

*5;[9] *accord Arnold*, 533 F.3d at 1008 ("[R]easonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."); *United States v. Linarez-Delgado*, 259 Fed. Appx. 506, 508 (3d Cir. 2007) ("Customs Officers exercise broad authority to conduct routine searches and seizures for which the Fourth Amendment does not require a warrant, consent, or reasonable suspicion . . . . Data storage media and electronic equipment, such as films, computers devices, and videotapes, may be inspected and viewed during a reasonable border search."); *Cancel-Rios v. United States*, No. 10-1386, 2010 WL 3420805, at *3 (D.P.R. Aug. 30, 2010) (border search of cell phone did not require reasonable suspicion); *United States v. Veema,* No. H-08-699-1, 2010 WL 1427261, *2-*3 (S.D. Tex. Apr. 8, 2010) (review of files on computer does not make a border search non-routine); *United States v. Bunty*, 617 F. Supp. 2d 359, 365 (E.D. Pa. 2008) (border searches of laptops "do not require reasonable suspicion"); *United States v. McAuley*, 563 F. Supp. 2d at 679 (holding "that the search of one's personal computer at a port of entry is a routine search and thus, does not necessitate a finding of reasonable suspicion"); *United States v. Pickett*, No. 07-374, 2008 WL 4330247, *3-*4 (E.D. La. Sept. 16, 2008)("search of his laptop and electronic devices was a non-invasive routine search that did not require reasonable suspicion"), *aff'd*, 598 F.3d 231 (5th Cir. 2010) ; *United States v. Hampe*, No. CR 07-3-B-W, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007) (Report and Recommendation holding that a search of computer at border "did not implicate any of the serious concerns that would justify characterizing this particular search as 'non-routine'"), *adopted*, 2007 WL 1806671 (D. Me. June 19, 2007).

---

[9] In upholding the district court's decision, the Second Circuit found that the customs agents who searched Irving had reasonable suspicion and thus did not consider whether reasonable suspicion was required. *Irving*, 452 F.3d at 124.

Plaintiffs' argument that electronic devices should be treated differently than other closed containers due to their ability to store large amounts of personal information (*See* Compl., ¶ 3) has been consistently rejected as contrary to both Supreme Court precedent and common sense. *See e.g., Arnold*, 533 F.3d at 1009; *McAuley*, 563 F. Supp. 2d at 677-78. As the Ninth Circuit observed, "the Supreme Court has refused to draw distinctions between containers of information and contraband with respect to their quality or nature for purposes of determining the appropriate level of Fourth Amendment protection." *Arnold*, 533 F.3d at 1009; *see also id.* at 1008 (district court erred in attempting to distinguish laptop computers from other pieces of property, such as the vehicle at issue in *Flores-Montano*); *McAuley*, 563 F. Supp. 2d at 677-78 (refusing to "impute the same level of privacy and dignity afforded to the sovereignty of a person's being to an inanimate object like a computer," and recognizing that "[a] computer is simply an inanimate object made up of microprocessors and wires which happens to efficiently condense and digitize" written information, such as Social Security cards, medical records, and day planners, is already subject to routine border searches).

Moreover, Plaintiffs' focus on the ability of electronic devices to store large amounts of personal information misses two vital points. First, the fact that a container may contain a large amount of personal items or information does not negate the fact that such containers also are capable of holding vast amounts of non-personal information. Moreover, accepting Plaintiffs' argument would lead to the perverse result that the more an item may contain dangerous amounts of information, the less authority under the Constitution customs officials would have to search the item. Under that view, smugglers and terrorists would have an obvious and overwhelming incentive to transfer their contraband onto a computer before bringing contraband into the country. Second, many other forms of containers subject to routine border search hold personal

items or information. For example, thousands of suitcases and other containers cross the border each day, and clearly many contain highly personal items such as photographs, medicines, underwear, contraceptive devices, and personal papers (*e.g.*, diaries, letters, tax information). A rule requiring the Government to have reasonable suspicion before conducting a border search of a container that may contain personal items or information would thus implicate such searches that have long been viewed as proper even though conducted without suspicion.

The Ninth Circuit, sitting *en banc*, emphasized the adverse consequences of placing imprudent constraints on the exercise of border search authority in a case involving the search of outbound packages and letters. *See United States v. Seljan*, 547 F.3d 993, 1005 n.9 (9th Cir. 2008) (*en banc*), *cert. denied*, 129 S. Ct. 1368 (2009). The court rejected an argument that customs officers must have reasonable suspicion to conduct such searches, stating:

> In a different context, it is not difficult to imagine that such an imprudent constraint could have disastrous consequences: To avoid detection, a terrorist could simply enclose in a separate sealed envelope within the FedEx package plans for an explosive device, instructions for an attack, the chemical formula for some form of poison, or any other type of document that could, under Seljan's proposed rule, qualify as unsearchable. Not only is such a rule unsupported under the law, it is unwise. *See* [*United States v.*] *Cortez-Rocha*, 394 F.3d [115,] 1123-24 [(9th Cir. 2005)] (underscoring the "importance of our policing borders . . . which at this juncture in our history is surely a pressing national special need" in view of the findings of the 9/11 Commission on terrorist travel) (internal quotation marks omitted).

547 F.3d at 1005 n.9.

Courts also have recognized that affording special constitutional protection for electronic devices "effectively would allow individuals to render graphic contraband, such as child pornography, largely immune to border search simply by scanning images onto a computer disk before arriving at the border." *Irving*, 2003 WL 22127913, at *5; *see also United States v. Ickes*,

393 F.3d 501, 506 (4th Cir. 2005) (recognizing that to "create a sanctuary at the border for all expressive material – even for terrorist plans . . . would undermine the compelling reasons that lie at the very heart of the border search doctrine"). In short, border searches of electronic devices without individualized suspicion do not violate the Fourth Amendment.

Plaintiffs' challenges to the Defendants' policies allowing detention for a reasonable period of time and copying of electronic devices in order to complete a border search likewise have no merit. The challenged policies provide that electronic devices may be detained for a reasonable period of time to perform a border search. *See* CBP Directive, ¶ 5.3.1; ICE Directive, ¶ 8.3(1).[10] The Fourth Amendment does not set arbitrary limits on the permissible duration of a border search; indeed, "the Supreme Court has 'consistently rejected hard-and-fast time limits' in evaluating the reasonableness of border searches and has stressed that 'common sense and ordinary human experience must govern over rigid criteria.'" *Tabbaa v. Chertoff*, 509 F.3d 89, 100 (2d Cir. 2007) (quoting *Montoya de Hernandez*, 473 U.S. at 543).

As courts have recognized, the process of searching the files in a computer or other electronic device "can take a long time" since, as Plaintiffs acknowledge, such devices may contain many files. *See United States v. Hill*, 459 F.3d 966, 974 (9th Cir. 2006) (quoting *United States v. Hill*, 322 F. Supp. 2d 1081, 1089 (C.D. Cal. 2004)); *accord United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 40 (D. Conn. 2002) (searching a seized computer "could takes weeks or months"); *United States v. Mitchell*, No. CR407-126, 2007 WL 2915889, *11 (S.D. Ga. Oct 3, 2007) (Report and Recommendation) (search of computer "often takes

---

[10] Except as otherwise provided by the policies, if after the information is reviewed, no probable cause exists to seize it, the challenged policies provide that any electronic copies of the information must be destroyed, and any electronic devices returned. *See* CBP Directive, ¶ 5.3.1.2; ICE Directive, ¶ 8.5(1)(e).

considerable time . . . to analyze a storage device containing many gigabytes of data"), *adopted,* 2007 WL 3102167 (S.D. Ga. Oct. 22, 2007).[11] In many cases, evidence or contraband are not simply found in neatly organized files in obvious sequence:

> Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observers. Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled "flour" or "talcum powder." There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it.

United States v. Hill, 459 F.3d at 98 (quoting *United States v. Hill*, 322 F. Supp. 2d at 1090-91); *accord United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006) (government should not be required to trust an individual's self-labeling because "computer files are easy to disguise or rename"); *United States v. Triumph Capital Group, Inc.*, 211 F.R.D. at 62 (agent's comprehensive manual review of files was reasonable because "a computer user can mislabel or deliberatively label files to avoid detection"). Moreover, a search of information on a computer or other electronic storage device poses special difficulties because there is a risk that officers might damage or compromise a file by attempting to access the data. *United States v. Hill,* 459 F.3d at 974 (quoting *United States v. Hill*, 322 F. Supp. 2d at 1089). Because of this, experts often make a back-up copy of the contents before beginning their search. *Id.* Simply put, examining a computer is complicated and time-consuming.[12]

---

[11] The cases cited involve computers searched pursuant to a warrant, but the language regarding the time it can take to search a computer is relevant to border searches as well.

[12] The Federal Rules of Criminal Procedure recognize this point. As the Advisory (continued...)

The fact that a search of a computer is made pursuant to the border search doctrine rather than pursuant to a warrant does not make the search any less difficult or time-consuming. As explained *supra* at 3, CBP and ICE have the responsibility for enforcing a wide range of laws, including laws relating to terrorism, narcotics, immigration, child pornography, money laundering, copyrights and trademarks, and export controls. Searches of electronic devices are "a crucial tool for detecting" violations of these laws. ICE Directive, ¶ 4; *see also* CBP Directive, ¶ 1. Border searches of computers present many of the same problems presented by searches of computers pursuant to a warrant. For example, as in the case of a computer subject to a warrant search, a computer user can mislabel files to avoid detection at the border. In view of these difficulties, permitting officers to detain and copy a laptop or other electronic device to complete a routine border search does not violate the Fourth Amendment.[13]

---

[12](...continued)
Committee notes, "[c]omputers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information . . . at the search location." *See* Fed. R. Crim. P. 41(e), Adv. Comm. Notes to the 2009 Amds. Moreover, as the Advisory Committee explains, "[a] substantial amount of time can be involved in the forensic imaging and review of information" in computers and other electronic devices "due to the sheer size of the storage capacity of media, difficulties created by encryption and boobytraps and the workload of the computer labs." *Id.* For this reason, the Federal Rules of Criminal Procedure have rejected "a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place." *Id.*

[13] In *United States v. Cotterman*, 2009 WL 465028, at *4-*5 (D. Ariz. Feb. 24, 2009), *appeal pending* Case No. 09-10139 (9th Cir.), a district court suppressed evidence of production and possession of child pornography found during a search of electronic devices detained at the border, but forensically examined by an ICE Field Office approximately 170 miles away from the point of detention. The search took approximately 48 hours to complete. The court held that this forensic analysis was not a routine border search, but instead an "extended border search," requiring a showing of reasonable suspicion, because of the time and distance involved. Based on that finding, the district court found that ICE and CBP lacked the reasonable suspicion required to justify an extended border search. This finding that the time and distance involved made the search an "extended border search" is fundamentally flawed and is inconsistent with
(continued...)

Thus, the challenged policies do not authorize or purport to authorize searches that would violate the Fourth Amendment. To the contrary, the policies contain safeguards to protect the privacy of travelers such as plaintiffs which are above and beyond that required by the Fourth Amendment. *See supra* at 5-8. Plaintiffs, therefore, are unable to show that there is "no set of circumstances exists under which the [policies] would be valid." *Flores*, 507 U.S. at 301. Accordingly, Plaintiffs' Fourth Amendment claims should be rejected.

B. The Policies Do Not Violate the First Amendment.

Plaintiffs' First Amendment challenge to the policies also fails as a matter of law. An otherwise valid search under the Fourth Amendment does not violate the First Amendment rights of an individual – even a completely innocent individual – simply because the search uncovers expressive materials. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 563-68 (1978).[14] This premise is equally applicable in the border search context. In *United States v. Borello*, 766 F.2d 46 (2d Cir. 1985), the Second Circuit recognized that the search and seizure of films that were "not legally obscene" in the course of a "reasonable border search" did not implicate the First Amendment. *Id.* at 58 ("Surely, Customs officials can permissibly screen [expressive] materials

---

[13](...continued)
Second Circuit caselaw. As a legal matter, a "border search" of a person's personal property is not complete until the personal property *clears* customs. *See United States v. Gaviria*, 805 F.2d 1108, 1112 (2d Cir. 1986); *accord United States v. Bareno-Burgos,* 739 F. Supp. 772, 778-79 (E.D.N.Y 1990) (Raggi, J.). An "extended border search," on the other hand, is a search "conducted after a person or some property has 'cleared an initial customs checkpoint and [has] entered the United States.'" *Gaviria,* 805 F.2d at 1112 (quoting *United States v. Glaziou*, 402 F.2d 8, 13 (2d Cir. 1968)). Because the devices in *Cotterman* had not cleared customs, the district court erred in finding that an extended border search had occurred.

[14] In response to *Zurcher*, Congress enacted the Privacy Protection Act, which generally prohibits the search or seizure of "any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. § 2000aa. Congress explicitly exempted customs and border searches from this prohibition. *See* 42 U.S.C. § 2000aa-5.

entering the country to enforce [criminal] laws.").

There is no basis to apply a different rule to the search of electronic devices. Indeed, both the Fourth and Ninth Circuits have squarely rejected attempts "to carve out a First Amendment exception to the border search doctrine" in the context of laptop searches. *See Ickes*, 393 F.3d at 506; *Arnold*, 533 F.3d at 1010. As these courts observed, such an exception would:

> (1) protect terrorist communications "which are inherently expressive"; (2) create an unworkable standard for government agents who "would have to decide—on their feet—which expressive material is covered by the First Amendment"; and (3) contravene the weight of Supreme Court precedent refusing to subject government action to greater scrutiny with respect to the Fourth Amendment when an alleged First Amendment interest is also at stake.

Arnold, 533 F.3d at 1010 (quoting *Ickes*, 393 F.3d at 506-08). Plaintiffs' First Amendment challenge to DHS's policies must be rejected for the same reasons.

III. THE BORDER SEARCH OF ABIDOR'S ELECTRONIC DEVICES DID NOT VIOLATE THE FIRST AND FOURTH AMENDMENTS.

Plaintiff Abidor also fails to state a claim with respect to the May 2010 border search of his laptop and external hard drive.[15] In his complaint, he alleges that the CBP officer searched his laptop when he crossed the border and detained his laptop and external hard drive for eleven days for ICE analysis. *See* Compl., ¶¶24-54. During this time, he alleges that Defendants made a copy of the contents of his laptop and external hard drive. *See id.*, ¶ 52.[16] He further alleges "on

---

[15] While the Complaint contains various allegations that CBP officials questioned Abidor for three hours, subjected him to a pat-down search, and took his photograph and fingerprints, Abidor does not claim that any of these actions were unconstitutional. Indeed, he cannot. Courts have repeatedly found that such questioning, searches, photographing and fingerprinting are routine and do not raise a cognizable constitutional claim. *See, e.g.*, *Tabbaa*, 509 F.3d at 98-99.

[16] For purposes of this motion only, Plaintiffs' allegations are assumed as true, including his implicit allegation that Defendants had no reasonable suspicion that his electronic devices

(continued...)

information and belief" that Defendants continue to possess "copies of the contents of [his] laptop and information derived from his devices." *Id.*, ¶ 54. He claims that this search, detention, and copying of his electronic devices violated the Fourth and First Amendments. *See id.*, ¶¶ 130-131. As a remedy, he seeks a declaratory judgment and order requiring Defendants to return or destroy "all information unlawfully retained." *Id.*, Prayer for Relief, C, F.

A. Abidor's Fourth Amendment Claim Should Be Dismissed.

Like Plaintiffs' facial challenges to the policies, these claims are predicated on the assumption that Defendants must have reasonable suspicion to search a laptop or other electronic devices at the border. As explained above, courts have found that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border." *Arnold*, 533 F.3d at 1008; *see supra* at 20-21. Abidor offers no reason why a different standard should apply to him.

Nor can Abidor establish that the eleven-day detention and any suspected copying of the contents of his laptop or external hard drive violated the Fourth Amendment. As explained above, the Fourth Amendment does not set arbitrary limits on the permissible duration of a routine border search. *See supra* at 24-26. Instead, "the Supreme Court has 'consistently rejected hard-and-fast limits' in evaluating the reasonableness of border searches and has stressed that 'common sense and ordinary human experience must govern over rigid criteria.'" *Tabbaa*, 509 F.3d at 100 (quoting *Montonya de Hernandez*, 473 U.S. at 543). For example, in *United States v. Gaviria*, a shipment of canned fruit arrived and was inspected by customs officers at Miami. *See* 805 F.2d at 1110. Miami customs officers did not see anything suspicious about the shipment, and the cartons

---

[16](...continued)
contained contraband or evidence of a crime.

were transported to JFK Airport, its ultimate destination, by a bonded truck carrier. *Id.* Three days after the cartons arrived at JFK, and eight days after their initial entry into the United States, Customs inspectors again examined the cartons and found cocaine. *Id.* The Second Circuit found that the search at JFK was a valid border search. *Id.* at 1111. Similarly, in *United States v. Gowadia*, 610 F. Supp. 2d 1234, 1242-43 (D. Haw. 2009), the court found that the search of a container to be a valid border search where the container had been set-aside for further examination but not examined until five days later.

Courts have recognized that searching files in a computer or other electronic devices can be complicated and time-consuming. *See supra* at 24-26. In order to avoid damage to the files, such a search often requires copying and review at another site by computer specialists. *See United States v. Hill*, 459 F.3d at 975 (quoting *United States v. Hill*, 322 F. Supp. 2d at 1089) ("[T]here is a serious risk that police might damage the storage medium or compromise the integrity of the evidence by attempting to access the data at the scene."). Moreover, taking the time needed to search a computer at the scene would "impose a significant and unjustified burden" on government resources. *Id.* at 975. Recognizing these difficulties, the ICE Directive states that "[s]earches are generally to be completed within 30 calendar days of the date of detention, unless circumstances exist that warrant more time." ICE Directive, ¶ 8.3(1). The eleven-day detention of the electronic devices for ICE's analysis here was much less that the thirty-day guideline set forth in the ICE Directive.

In short, Abidor cannot state a Fourth Amendment claim based on the search, detention, and purported copying of his laptop.

B. Abidor's First Amendment Claim Should Be Dismissed.

Abidor's First Amendment claim with respect to the search of his electronic devices also

fails as a matter of law. As explained *supra* at 27-28, the fact that his laptop and external hard drive contained expressive material does not make the search invalid. In *United States v. Borello,* 766 F.2d at 58, the Second Circuit specifically recognized the right of customs officials to look at expressive materials. Moreover, the Fourth and Ninth Circuit have rejected similar First Amendment claims with respect to border searches of electronic devices. *Ickes*, 393 F.3d at 506; *Arnold*, 533 F.3d at 1010.

Abidor's claims with respect to the search, detention and purported copying of his laptop and other electronic devices should, therefore, be dismissed for failure to state a claim.

CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court grant their Motion to Dismiss.

Respectfully submitted,

TONY WEST
Assistant Attorney General

LORETTA E. LYNCH
United States Attorney

ELLIOT M. SCHACHNER
Assistant U.S. Attorney

SANDRA M. SCHRAIBMAN
Assistant Branch Director

s/Marcia Sowles
MARCIA SOWLES
Senior Counsel
U.S. Department of Justice, Civil Division
Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7114
Washington, D.C. 20530
Tel.: (202) 514-4960
Fax.: (202) 616-8470

Email: marcia.sowles@usdoj.gov